Eve H. Cervantez (164709)
Jonathan Weissglass (185008)
ALTSHULER BERZON LLP
177 Post Street, Suite 300
San Francisco, CA 94108
Telephone: (415) 421-7151
Facsimile: (415) 362-8064

Attorneys for Plaintiff and the Proposed Class

(*Additional counsel appear on signature page*)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

KATHRYN LENISKI, individually and on behalf of all others similarly situated, Plaintiff, v. ANTHEM, INC., d/b/a Anthem Health, Inc., an Indiana Corporation, THE ANTHEM COMPANIES, INC., an Indiana Corporation and BLUE CROSS OF CALIFORNIA, d/b/a Anthem Blue Cross, a California Corporation, Defendants.	Case No.: 15-2992 CLASS ACTION **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

TABLE OF CONTENTS

1. Defendants Anthem, Inc. d/b/a Anthem Health, Inc., The Anthem Companies, Inc., and Anthem, Inc.'s subsidiary, Blue Cross of California, d/b/a Anthem Blue Cross (collectively "Anthem" or "Defendants") are national health insurers with computer systems that store highly sensitive and highly confidential information about current and former customers and employees, including social security numbers ("SSNs"), names, addresses, dates of birth, medical records and financial information, which they are required and duty bound to safeguard from unauthorized disclosure and theft. Plaintiff Kathryn Leniski seeks remedies on behalf of herself individually and on behalf of a Nationwide Class, as defined below, resulting from Defendants' failures to adhere to their cyber-security and medical records data and information duties and responsibilities resulting in and associated with a data breach affecting many millions of past and present customers, and their failure to *immediately* and *accurately* notify such past and current customers and employees in order to prevent them from becoming victims of or otherwise being damaged by identity theft. The facts and information alleged herein are based upon an investigation by counsel. Plaintiff believes that further substantial evidentiary support for the allegations herein will exist after a reasonable opportunity for further investigation and discovery. In support of this complaint against Defendants, Plaintiff alleges on information and belief as follows:

I. INTRODUCTION

2. On February 4, 2015, Anthem disclosed for the first time that hackers had breached its database containing highly confidential medical records and personal private information, including member IDs and social security numbers, of many millions of its current and former customers, including federal government personnel and Defendants' employees. Anthem – the parent company of Anthem Blue Cross and Blue Shield and the second largest health insurer in the United States – was responsible for maintaining the security and integrity of the medical records and personal information it possessed regarding its insureds.

3. The hacking, adversely affecting millions of innocent customers insured by Anthem in return for the payment of health care premiums, never should have occurred and was

a result of Anthem's willful misconduct and recklessness in the face of a known serious risk and danger. The massive data breach could have and should have been prevented, especially given that Anthem and the health care industry had been previously placed on alert in 2014 by the United States Federal Bureau of Investigation of the increasing risk and threat to them from criminal hackers and that Anthem's predecessor, Wellpoint, experienced a prior cyber-attack, which exposed the weaknesses in its cyber-security practices and data security systems.

4. Anthem knew at all times material that it possessed highly confidential, private and personal data and information about its customers and insureds and that hacking into its data banks was a clear risk respecting which it had a moral, legal, statutory and self-imposed duty to adequately guard against in order to protect innocent victims from data breach or theft. Anthem was also aware that many of its insureds and customers are federal government employees, including individuals in key or sensitive positions in federal agencies and certain branches of government. Generally speaking, such customers and insureds have well founded concerns regarding their personal cyber-security. Despite this, Plaintiff is informed and believes and thereupon alleges that Anthem failed to take the necessary steps that it reasonably could have taken to protect its data storage systems from an attack and resulting breach.

5. One reasonable method of protecting the personal and confidential data and information from criminal enterprises and hackers seeking to access such valuable records, including social security numbers, and stealing identities, is well known: "encryption." Safeguarding Anthem and its tens of millions of member insureds from identity theft as a consequence of criminal hacking required the building of "strong walls" around and likely within customer databases and pieces of data, and "strong doors" that allowed information to be accessed through such walls only by those who truly and legitimately needed it and no one else. Plaintiff is informed and believes and thereupon alleges that despite the known extreme risk of hacking, Anthem, among other things, failed to appropriately encrypt its customers' and insureds sensitive and personal data in its possession from identity theft of information patients were necessarily required to divulge to their health care providers and, in turn, to Anthem, in order to receive the

benefits from Defendants that they or their employers paid for. Instead, Anthem effectively left open the door to a vault of highly valuable and personal information it was obliged to safeguard, in part because it placed its own corporate goal of improving its bottom line financial performance by implementing effective cost controls ahead of its responsibility to safeguard and protect its former and current customers' identities and confidential information from theft.

6. As a result, Anthem, which claimed net income of approximately $2.6 billion in 2014, has enabled criminal enterprises and hackers to secure a treasure trove of personal information, including millions of social security numbers – described as "the key that unlocks the vault" – exposing millions of customers to identity theft and other harmful consequences and damage. These customers and insureds, including federal government employees and their dependents, consequently live in a state of cyber-insecurity.

7. Anthem never fully, adequately or timely disclosed that it had failed to adequately protect its current or former customers from identity theft. And, further reflecting an utter disregard for the security and safety of the personal information it was duty bound to secure and protect, Anthem failed to timely notify the individual victims of the data breach even while identity thieves were free to go about their business of exploiting the information for profit, including selling it on the black market. As Paul Stephens of the Privacy Act Risks Clearinghouse has reportedly stated: "This is one of the worst breaches I have ever seen … these people knew what they were doing and recognized there was a treasure trove here … they are going to use it to engage in very sophisticated kinds of identity theft." In turn, Plaintiff and members of the Class risk identity theft caused by Anthem's profound lack of data security systems and control and are faced with expending monies to try and protect themselves, albeit too late given Anthem's untimely notice.

II. JURISDICTION AND VENUE

8. This Court has federal question jurisdiction, 28 U.S.C. §1331, because this action arises under the laws of the United States, including the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.* This Court also has diversity jurisdiction over this action under the Class Action

Fairness Act, 28 U.S.C. §1332. The proposed class consists of 100 or more members and the aggregated claims of the individual Class Members exceed the sum or value of $5,000,000 exclusive of costs and interest. Additionally, at least one class member is a citizen of a state that is different than the Defendants'.

9. Venue is proper in this Court pursuant to 28 U.S.C. §1391(b) because Anthem regularly conducts business in this District, some of the Class Members reside within this District, and because this case is related to other substantially identical class actions that have been filed against the Defendants in this District. Many of the unlawful practices respecting Anthem's cyber-security, as complained of below, occurred as a result of decisions made or implemented by Anthem in conjunction with its cyber-security consulting firm which is located within this District in Milpitas, Santa Clara County, California.

III. INTRADISTRICT ASSIGNMENT

10. Pursuant to Civil L.R. 3-2(c) and 3-5(b), assignment to the San Jose Division of the Northern District of California (the "Division") is proper, because a substantial part of the events or omissions which give rise to the claims occurred in this Division. Defendants sell health insurance plans in this Division, maintain offices in this Division, employ workers in this Division, and advertise in this Division. Many of the unlawful practices respecting Anthem's cyber-security, as complained of below, occurred as a result of decisions made or implemented by Anthem in conjunction with its cyber-security consulting firm which is located within this Division in Milpitas, Santa Clara County, California. Assignment to the San Jose Division is also proper because cases relating to the Anthem data breach have been centralized before the Honorable Lucy Koh by the Judicial Panel on Multidistrict Litigation as *In re Anthem, Inc. Customer Data Breach Security Litig.*, No. 5:15-md-02617-LHK (N.D. Cal.)

IV. PARTIES

Plaintiff

11. Plaintiff Kathryn Leniski ("Leniski") is a resident of Mishawaka, Indiana, and has been and is a health insurance customer of Anthem. Ms. Leniski first joined an Anthem health

plan in or about 2010. For the period of 2013-2014 she was enrolled in the "Anthem-Blue Cross Blue Shield Luminous Plan." For 2015 she has been enrolled in the "Anthem Bronze Pathway X" health insurance plan.

12. Plaintiff Kathryn Leniski is one of the many victims of the Anthem cyber-attack and breach. The damage that she has suffered is continuing.

13. On March 2, 2015, Plaintiff Leniski received a letter from the Indiana Department of Revenue directing her to call the agency to confirm her identity and receive her "tax refund." But Ms. Leniski had not yet filed her 2014 Indiana State Tax Return as of March 2, 2015.

14. Upon further inquiry, the agency advised Ms. Leniski that her identity had been compromised: someone had filed her 2014 tax return without her knowledge in an effort to steal any tax refund. Ms. Leniski was advised by the agency to file a formal fraud report with the St. Joseph's County Police. Thereafter, Ms. Leniski spent 3 full days visiting with State and Federal investigators (FBI, IRS). She missed a work day, costing her $150 in lost wages, and incurred transportation expenses.

15. On March 8, 2015, Ms. Leniski received a letter from Anthem providing notice of the data breach of Anthem and consequent possibility that her employment data had been compromised. And as a consequence of the investigation they were conducting, Ms. Leniski was informed by the Department of Revenue that the attempted fraud respecting any 2014 state tax refund likely resulted from the Anthem breach.

16. Plaintiff Leniski is informed and believes and on that basis alleges that as a direct and proximate cause of the Anthem data breach, a tax refund of $2,200.00 owed to her was delayed, her credit cards were declined and frozen and her credit was impaired. Ms. Leniski must now incur additional costs to protect her identity and to guard against cyber-theft going forward, all the while mindful that her highly personal social security number is in adverse hands, along with other confidential personal information, creating a significant risk of her being further victimized by cyber-fraud and theft throughout the balance of her life.

Defendants

17. Defendant Anthem, Inc., doing business as Anthem Health, Inc., is an Indiana corporation registered with the California Secretary of State to do business in California and headquartered at 120 Monument Circle, Indianapolis, IN. Defendant The Anthem Companies, Inc. is an Indiana corporation, registered with the California Secretary of State to do business in California with its corporate headquarters in Indianapolis, IN. Through its subsidiary Anthem Insurance Companies, Inc., also an Indiana corporation, Anthem, Inc. provides healthcare benefits through Blue Cross and Blue Shield plans in California, Colorado, Connecticut, Georgia, Indiana, Kentucky, Maine, Missouri, Nevada, New Hampshire, New York, Ohio, Virginia and Wisconsin. In December 2014, WellPoint, Inc. changed its name to Anthem, Inc.

18. Defendant Blue Cross of California, d/b/a Anthem Blue Cross, is a California corporation that is an independent licensee of the Blue Cross Association. Blue Cross of California's parent company is Anthem, Inc.

19. Defendant Anthem, Inc., The Anthem Companies, Inc., and Blue Cross of California are collectively referred to herein as "Defendants" or "Anthem," unless noted otherwise.

V. FACTUAL ALLEGATIONS

A. A Booming and Lucrative Market for Hackers

20. According to experts, medical identity theft is on the rise because it pays. In black-market auctions, complete patient medical records tend to fetch higher prices than credit card numbers. One security expert said that at one auction a patient medical record sold for $251, while credit card records were selling for $0.33.

21. Underground hacker markets are booming. According to an article published in December 2014 by DELL SecureWorks, Underground Hacker Markets, the most significant difference between the 2014 underground hacker market and those of 2013 is that the markets are booming with counterfeit documents to further enable fraud, including new identity kits, passports, utility bills, social security cards and drivers licenses. The underground hacker markets

are monetizing every piece of data they can steal or buy and are continually adding services so other scammers can successfully carry out online and in person fraud.

22. Statistics maintained by the United States Department of Human Services say there have been 740 major health care breaches affecting 29 million people over the last 5 years. According to Katherine Keith, a global focus group leader for breach response services at insurer Beazley, which underwrites cyber liability policies, health care companies are attractive targets to hackers because of the wealth of sensitive personal information maintained in their networks. Indeed, such information about customers tends to be more valuable on the black market than the credit card information that is often stolen from a retailer. Hence, the combination of social security information and a patient's medical history constitutes a valuable commodity to criminals. Stolen medical information can also be used to make false insurance claims.

B. A Critical Need to Secure and Protect Data from Breach in the Healthcare Industry

23. Health care companies are required to maintain the security of their customers' personal, health, and financial information. Anthem itself recognizes this important obligation in its HIPAA Notice of Privacy Practices handbook where it addresses the consumers' "protected health information" or "PHI":

> We keep the health and financial information of our current and former members private, as required by law, accreditation standards and our rules.
> …
> We are dedicated to protecting your PHI, and have set up a number of policies and practices to help make sure your PHI is kept secure. We keep your oral, written and electronic PHI safe using physical, electronic, and procedural means. These safeguards follow federal and state laws. Some of the ways we keep your PHI safe include securing offices that hold PHI, password Protecting computers, and locking storage areas and filing cabinets....

24. According to a report in *The New York Times* "[t]he threat of a hacking is particularly acute in the health care and financial services industry, where companies routinely

keep the most sensitive personal information about their customers on large databases."[1]

25. The push to digitized patient health records in hospitals and doctors' offices has also made medical records increasingly vulnerable. According to security experts, moving medical records from paper to electronic form has made patient records more susceptible to breaches, including criminal attack. "The healthcare industry has become, over the last three years, a much bigger target," according to Daniel Nutkis, the Chief Executive of Health Information Trust Alliance, an industry group that works with healthcare organizations to improve their data security.[2] Despite this, healthcare providers have lagged far behind other industries according to experts. "When we go to a healthcare show and you look at the screens of different systems, it's like we're looking at Windows XP," said Bob Janecek, a co-founder and chief technology officer of DataMotion, an email encryption and health information service provider. "When you go to a banking show and they're talking about how to slice a billionth off a second off a transaction to get a competitive edge, it's just totally different."[3]

26. Healthcare companies, including Anthem, were specifically warned by the Federal Bureau of Investigation in 2014 of the increasing threat to them from hackers.

27. On April 8, 2014, the FBI's Cyber Division issued a public Private Industry Notification titled "Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain." The notification specifically cautioned that "[c]yberactors will likely increase cyber intrusions against health payout for medical records in the black market."

28. The FBI cited a report issued in February 2014 by SANS, a leading computer forensics and security firm, warning:

> Health care security strategies and practices are poorly protected and ill-equipped to handle new cyber threats exposing patient medical records, billing and payment organizations, and intellectual property .... The biggest vulnerability was the

[1] http://www.nytimes.com/2015/02/05/business/hackers-breached-data-of-millions-insurer-says.html (last accessed Feb. 5, 2015).

[2] http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html (last accessed Feb. 12, 2015).

[3] http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html (last accessed Feb. 12, 2015).

perception of IT health care professionals' beliefs that their current perimeter defenses and compliance strategies were working when clearly the data states otherwise.

29. By early 2014, it was well known, inside and outside the healthcare sector, that computer breaches had become rampant in the healthcare industry. According to a Ponemon Institute report dated March 2013, 63% of the healthcare organizations surveyed reported a data breach during the previous two years. The majority of these breaches resulted in the theft of data. In a March 2014 report, the institute stated that criminal attacks on healthcare companies had increased 100% since 2010. An EMC2IRSAWhite Paper published in 2013 indicated that during the first half of 2013, more than two million healthcare records were compromised, which was 31% of all reported data breaches. According to the Identity Theft Resource Center, nearly half of all data breaches so far in 2014 have taken place in the healthcare sector. According to analysis of HHS data by the *Washington Post's* "Wonkblog," the personal data of about 30.1 million people has been affected by 944 recorded "major" health data breaches (defined by HHS as one affecting at least 500 people) since federal reporting requirements under the 2009 economic stimulus package went into effect.

30. Studies have shown that the healthcare industry is one of the most affected by and least prepared to deal with hacking attempts. Despite the growing threat, the healthcare industry has been slow to implement improved security measures – slower than other industries handling sensitive information, such as the retail and financial sectors. For instance, the typical healthcare entity allocates only about 2 or 3 percent of its operating budget to its IT department, while retail and financial businesses devote more than 20 percent to IT. According to an annual security assessment conducted by the Healthcare Information and Management Systems Society, almost half of surveyed health systems said they spent 3 percent or less of their IT budgets on security.

C. The Cyber-Threat to America's Government Employees and Families

31. Anthem provides services to the federal government in connection with its Federal Employee Program ("FEP") and various MediCare programs. FEP members consist of United States government employees and their dependents within Anthem's geographic markets through

its participation in a national contract between BCBSA and the U.S. Office of Personnel Management. Anthem, through its participation in various federal government programs, generated approximately 21%, 20.3% and 23.7% of its total consolidated revenues from agencies of the United States for the years ending December 31, 2014, 2013 and 2012 respectively.

32. Government employees and their dependents are another target of cyber thieves and hackers – and especially foreign states or agencies whose interests are not aligned with America's. According to a February 6, 2015 article *New York Times* entitled "Data Breach at Anthem May Forecast a Trend" – which was published before a massive hack of the United States government in May 2015 – "the key is the hackers' motive." Hackers "may also be searching for intelligence on government officials or senior executives who mask their personal information, but tend to provide real names and real numbers when dealing with health related matters. "The question is whether this is about espionage or theft," said one government official. Irrespective of any espionage, government employees are exposed to cyber-insecurity, especially in the case of Anthem. This presents an array of personal issues, concerns and security risks that can arise from a cyber-attack that Anthem knew and had reason to know its failure to provide cyber-security best practices could create.

D. Anthem Knew the Grave Risk of Data Breach and Need for Protection

33. As the second largest healthcare insurer in the United States, Anthem knew full well that it was at grave risk of being hacked. In fact, it had been hacked before. In or around October 2009, WellPoint, now known as Anthem, installed new hardware on certain of its web-based servers that store electronic versions of certain applications for health benefit coverage and other personal identifying information and personal health information associated with those applications belonging to its customers, enrollees or subscribers. The username, password and encryption security protections were not provided with the upgraded web servers and, as a result, the electronically stored personal information and personal health information of WellPoint customers, enrollees or subscribers was unprotected, as a consequence of which, between October 23, 2009 through and around March 10, 2010, a significant breach of WellPoint's data security

occurred. WellPoint thereafter contended that it implemented protections on or about March 10, 2010 and remediated the vulnerability of its system. But – and as Anthem knew and in the exercise of reasonable diligence should have known – WellPoint had failed to secure its data with appropriate encryption and other data system controls.

34. Subsequently, WellPoint, now known as Anthem, paid a $1.7 million penalty to the United States Department of Health and Human Services (HHS) as a consequence of that breach. The agreement that was reached between WellPoint and HHS stated several findings from the HHS investigation following what amounted to a Health Insurance Portability and Accountability Act ("HIPAA") violation. The HHS investigation report revealed that WellPoint had failed to implement appropriate security procedures and policies and violated HIPAA's security policies. It also failed to perform technical evaluations of system security following its software upgrade and failed to utilize adequate technology to identify users seeking access to sensitive information. Roy Mellinger, WellPoint's Chief information security officer at the time, is currently the chief information security officer for Anthem. The 2010 data breach experienced by WellPoint was not its first: it had also lost names, social security numbers (SSNs) and other data regarding 196,000 customers in 2007.

35. In 2012, Anthem Blue Cross disclosed SSN's on letters mailed to over 33,000 of its Medicare Supplement and Medicare Part D subscribers between April 2011 and March 2012 in violation of California law restricting their disclosure. The State of California ultimately sued the company in order to protect the privacy of Californians and reached a settlement of the action intending that such a privacy violation would not re-occur.

36. Anthem knew full well that the customer and employee information it maintained was not only highly sensitive but also highly valuable to identity thieves and has held itself out as adopting, maintaining, and being committed to data security policies it describes as follows:

> Personal Information (Including Social Security Number) Privacy Protection Policy
>
> Anthem Blue Cross and Blue Shield maintains policies that protect the confidentiality of personal information, including Social Security numbers, obtained from its members and associates in the course of its regular business

functions. Anthem Blue Cross and Blue Shield is committed to protecting information about its customers and associates, especially the confidential nature of their personal information (PI).

Personal Information is information that is capable of being associated with an individual through one or more identifiers including but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, and does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

• Anthem Blue Cross and Blue Shield is committed to protecting the confidentiality of Social Security numbers and other Personal Information.

• Anthem Blue Cross and Blue Shield's Privacy Policy imposes a number of standards to:

• guard the confidentiality of Social Security numbers and other personal information,
• prohibit the unlawful disclosure of Social Security numbers, and
• limit access to Social Security numbers.

Anthem Blue Cross and Blue Shield will not use or share Social Security numbers or personal information with anyone outside the company except when permitted or required by federal and state law.

Anthem Blue Cross and Blue Shield Associates must only access Social Security numbers or personal information as required by their job duties. Anthem Blue Cross and Blue Shield has in place a minimum necessary policy which states that associates may only access, use or disclose Social Security numbers or personal information to complete a specific task and as allowed by law.

Anthem Blue Cross and Blue Shield safeguards Social Security numbers and other personal information by having physical, technical, and administrative safeguards in place.

E. Anthem Did Not Adequately Secure Confidential Information or Protect it From Theft

37. Anthem was obliged to use every means available to it to protect private and confidential data including SSN's from falling into criminal hands. In truth, Anthem woefully failed to adopt and implement cyber-security best practices and even take rudimentary steps in certain respects. Anthem's data and records should have been properly and adequately encrypted.

Anthem should have built into its records platforms and cyber-security protocols "strong walls" and "strong doors" that would have thwarted cyber thieves. Anthem could have converted customers' and employees' confidential and sensitive information into coded strings that would not be immediately useful or identifiable to cyber-thieves. Instead, Anthem did not take all necessary steps regarding encryption. In many instances, it even chose to store highly sensitive and confidential information including social security numbers in plain text that would be readily identifiable and usable.[4]

38. Moreover, Anthem's data security system was not even consistent with healthcare industry standards required for the protection of sensitive information or health industry regulations as defined by HIPAA. HIPAA mandates that all protected health information – PHI – is required to be "protected," that an unauthorized disclosure of PHI is treated as a security incident (HIPAA Security Rule 45 C.F.R. Sess. 164.304) and that security incidents are met with a security incident response. HIPAA Security Rule CFR Sess. 164.308(a). The HIPAA Security Rule refers to several standard or recommended documents that are released by the National Institute of Standards and Technologies as methods to achieve HIPAA compliance. Federal Register Vol. 68, No. 34, at 8346,8350, 8352, 8355.

39. Anthem was not particularly concerned about protecting its former and current customers from identity theft. It was more concerned with its bottom line financial results and Wall Street's reaction to those results. On Thursday, February 5, 2015, after the Anthem data breach had been announced, Wall Street's reaction was essentially "ho-hum," with shares falling just $0.42 – less than a third of one percent. Wall Street basically shrugged off Anthem's example of corporate cyber-weakness as being almost meaningless. Unfortunately, it also evinced another concern – that companies viewed corporate security breaches as so frequent and ubiquitous that they have become little more than a routine cost of doing business.

40. "Companies are getting off relatively unscathed," said Paul Stevens, director of Policy and Advocacy for the Privacy Rights Clearinghouse in San Diego, adding, "they provide

[4] http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html (last accessed Feb. 12, 2015).

some credit monitoring to placate customers, but they have no real incentive to do better."[5] Businesses like Anthem harbor a reckless attitude that encrypting all data is simply too costly and cumbersome. It slows things down and harms productivity so they say. None of the data accessed by hackers in the various incidents that have occurred, including that of Anthem, was encrypted. Had the data been encrypted, the danger to consumers would have been lower or nonexistent.[6]

F. Confidential Customer and Employee Data Has Been Stolen Due to Anthem's Misconduct

41. On February 4, 2015, it was disclosed that hackers had stolen information on millions of Anthem customers, current and former, in a massive data breach that ranks among the largest in corporate history. The information stolen from the insurance giant includes names, birthdays, medical IDs, social security numbers, street addresses, email addresses and employment information including income data. The compromised database contained up to 80 million former and current customer records. CBS Moneywatch reported "not all data breaches are created equal and Anthem health insurance's hack is about as bad as they get for customers."[7]

42. Thomas Miller, Anthem's Chief Information Officer, has acknowledged that Anthem and other health care companies had become increasingly aware of the criminal value of the information that they possess in light of the large cyber attacks against financial service companies like JP Morgan and Chase and retailers like Target. Still, at the time of the data breach at Anthem, it had not yet encrypted its internal database or taken many other steps to improve its security.

---

[5] "Wall Street's reaction to Anthem data breach: ho-hum" http://www.latimes.com/business/la-fi-lazarus-20150206-column.html (last accessed February 12, 2015).

[6] "Wall Street's reaction to Anthem data breach: ho-hum" http://www.latimes.com/business/la-fi-lazarus-20150206-column.html (last accessed February 12, 2015).

[7] Mitch Lipka Anthem Data Breach: Steps You Need to Take available on 2.5.15 at http://www.cbsnews.com/news/what-you-need-to-know-about-the-anthem-hack/ (last accessed Feb. 12, 2015).

43. Anthem acknowledged on February 4, 2015 that the data that was accessed by hackers had not been encrypted, as is the normal practice of many companies. "When the data is moved in and out of the warehouses it is encrypted. But when it sits in the warehouse, it is not encrypted," Anthem spokeswoman Cindy Wakefield claimed. According to Richard Marshall, a former senior cyber security defense expert at the U.S. National Security Agency, Anthem should have encrypted the social security numbers. "Social security numbers can be sold to people that are here illegally … identity theft is a major issue." Anthem's admission that the information involved was not encrypted in its database, "drew immediate fire from some security experts" because "it is irresponsible for businesses not to encrypt the data."[8]

44. Encryption is a physical safeguard that can be extremely helpful to lowering cyber security risk. The failure to adequately encrypt the social security numbers and other private, confidential and highly sensitive information by Anthem is more than just alarming – it represents a wholesale and egregious failure to comply with its obligations, morally, ethically, as a matter of its own assumed and professed duties and under the law. Anthem consciously and deliberately failed to and chose not to encrypt.

1. The "Worst Kind of Data Breach" Causing "Mass Victimization of the Worst Kind"

45. Security experts characterize the intrusion into Anthem's system as imminently dangerous. The Indianapolis Star reports: "This is absolutely the worst kind of data breach, because thieves have stolen the information that's the most valuable, the most dangerous and impossible to change or cancel," said Neal O'Farrell, Credit Sesame's security and identity theft expert in an email. "This is mass victimization of the worst kind."[9]

46. Numerous tools exist that companies can deploy and this episode brings home the need for better protective measures, according to Benn Konsynski, George S. Craft professor of

[8] "Anthem hack exposes data on 80 million; experts warn of identity theft" http://www.latimes.com/business/la-fi-anthem-hacked-20150204-story.html#page=1 (last accessed Feb. 5, 2015).

[9] http://www.indystar.com/story/news/2015/02/05/anthem-data-breach-lifelong-battlecustomers/22953623

information systems and operations management at Emory University's Goizueta Business School. "The scale is enormous. I am sort of bewildered that we still have this magnitude of exposure," he said. "It certainly is the third or the fourth wake-up call to the market. ... (It) is incumbent on firms like that to go the extra mile to make sure that exposure is prevented or minimized in those processes.[10]

47. This was not your run of the mill hack. It is the holy grail of a hack. Because the data breach includes social security numbers and dates of birth, criminals can easily open credit in their names. If they had simply stolen a credit or debit card number, a consumer could just get a new card. But in this instance, they stole the skeleton key to someone's credit. In addition to selling Anthem customer data on the black market, fraudsters and thieves can use the data to set up financial accounts in victims' names, such as credit card accounts.[11] Criminals and others can apply for credit in that person's name, whenever they want, for as long as that person lives. The hack of Anthem is many multiple times worse than what occurred at Target and Home Depot combined. One's social security number does not change. One's date of birth does not change. These are the two primary means of creating a gateway to someone's credit and identity theft.

48. Victims of the Anthem data breach will undoubtedly suffer significant and ongoing financial harm. As Neal O'Farrell, a security and identity theft expert for CreditSesame.com states, "This time the crooks got social security numbers, for identity thieves, the social security number is the key that unlocks the vault and they now have millions of them."[12]

49. The Anthem breach is "one of the worst breaches" that has ever occurred according to Paul Stephens, director of Policy and Advocacy for the Privacy Rights Clearinghouse, a non-

---

[10] http://www.indystar.com/story/news/2015/02/05/anthem-data-breach-lifelong-battlecustomers/22953623

[11] http://www.cbsnews.com/news/how-hackers-might-use-your-stolen-anthem-data/ (last accessed Feb. 12, 2015).

[12] Mitch Lipka Anthem Data Breech: Steps You Need to Take available on 2.5.15 at http://ww.cbsnews.com/news/what-you-need-to-know-about-the-anthem-hack/ (last accessed Feb. 12, 2015).

profit consumer education and advocacy group. "These people knew… there was a treasure trove here and I think they are going to use it to engage in very sophisticated kinds of identity theft."[13]

2. The Anthem Data Breach Has Caused Severe, Long Term Adverse Effects

50. The type of information that the hackers have accessed from Anthem's IT systems could create problems for those affected for years to come. Privacy expert Rick Kam, president and co-founder of the Portland, Oregon-based company ID Experts, says: "Such information can be sold on the black market to open the door to a range of identity theft schemes. For instance, criminals have all the information they need to submit fraudulent tax returns[.]" Victims might not realize they have been affected until they try to process their returns.[14]

51. Or, a person could use the information to engage in medical identity fraud, said Ann Patterson, senior vice president and program director of the Medical Identity Fraud Alliance. Consumers need to carefully review all explanations of benefits they received from insurers to make sure that they have not been the victim of medical identity theft. Medical identity theft could inadvertently result in harm to the victim, Patterson added. For instance, if the perpetrator does not share the same blood type as the victim, a person could receive a dangerous transfusion.[15]

52. On February 6, 2015, Anthem posted a warning on its website that "Individuals who may have been impacted by the cyber attack against Anthem, should be aware of scam email campaigns targeting current and former Anthem members." "This outreach is from scam artists who are trying to trick consumers into sharing personal data."[16]

---

[13] http://www.nytimes.com/2015/02/06/business/experts-suspect-lax-security-left-anthem-vulnerable-to-hackers.html (last accessed Feb. 12, 2015).

[14] http://www.indystar.com/story/news/2015/02/05/anthem-data-breach-lifelong-battlecustomers/22953623

[15] http://www.indystar.com/story/news/2015/02/05/anthem-data-breach-lifelong-battlecustomers/22953623

[16] http://ir.antheminc.com/phoenix.zhtml?c=130104&p=irol-newsArticle&ID=2014520

53. Unlike credit card fraud, this episode may affect not just individuals but entire families. One individual expressed his fears as "lifelong":

> Greenwood resident John Sickmeier takes pains not to give out his or his five children's Social Security numbers. Whenever asked for this data on a form, he jots down a note, "Call for number." That way, he said, he restricts how many people have access to this information. The Anthem breach, which could include his children's Social Security numbers, could haunt them for years to come, he said. "What was stolen was far more threatening and egregious. It's everything that a thief would need to steal one's identity," Sickmeier said. "This could very well be a lifelong battle either for myself or any of my children."[17]

3. Investigation by Insurance Regulators

54. The National Association of Insurance Commissioners, a group of state insurance regulators, plans a multistate examination of Anthem. "We are in agreement that an immediate and comprehensive review of the company's security must be a priority to ensure protection of consumers who are covered by Anthem," said Monic Lindeen, the Association's president.[18] Several states are investigating the massive cyber attack stealing information belonging to many of millions of current and former customers as well as employees. Attorney Generals of Connecticut, Illinois, Massachusetts, Arkansas and North Carolina are looking into the breach, according to representatives of their offices and internal documents. And California's Department of Insurance said it will review Anthem's response to the data attack.

VI. CLASS ALLEGATIONS

55. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action as a national class action for herself and all members of the following Class of similarly situated individuals and entities:

The Nationwide Class

All persons in the United States whose personal information was compromised as a result of the data breach first disclosed by Anthem on February 4, 2015.

---

[17] http://www.indystar.com/story/news/2015/02/05/anthem-data-breach-lifelong-battlecustomers/22953623

[18] http://www.nytimes.com/2015/02/07/business/data-breach-at-anthem-may-lead-to-others.html (last accessed Feb. 10, 2015).

56. Excluded from the Class are Defendants, including any entity in which Defendant has a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants.

57. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of the claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

58. All members of the proposed Class are readily ascertainable. Anthem has access to addresses and other contact information for all members of the Class, which can be used for providing notice to Class members.

59. Numerosity. The Class is so numerous that joinder of all members is unfeasible and not practical. While the precise number of Class members has not been determined at this time, Anthem has admitted that 80 million records were stolen relating to past and current customers and employees, and it has over 37 million current health insurance customers.

60. Commonality. Questions of law and fact common to all Class members exist and predominate over any questions affecting only individual Class members, including, inter alia:

a. whether Anthem engaged in the wrongful conduct alleged herein;

b. whether Anthem's conduct was deceptive, unfair, and unlawful;

c. whether Anthem owed a duty to Plaintiff and members of the Class to adequately protect their personal, health, and financial information;

d. whether Anthem owed a duty to provide timely and accurate notice of the Anthem data breach to Plaintiff and members of the Class;

e. whether Anthem's conduct was likely to deceive a reasonable person;

f. whether Anthem used reasonable and industry-standard measures to protect Class members' personal information;

g. whether Anthem knew or should have known that its data system was vulnerable to attack;

h. whether Anthem's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of millions of consumers' personal, health, and financial data;

i. whether Defendants failed to timely disclose that they had not adequately secured their confidential financial and medical data, including failing to encrypt that data and/or their SSN's despite Defendants' knowledge of a grave threat of cyber-theft from its vulnerable system; and

j. whether Anthem timely and adequately notified the public after it learned of the data breach.

61. Typicality. Plaintiff's claims are typical of the claims of the Class. Plaintiff and all Class members were injured through the uniform misconduct described above and assert the same claims for relief.

62. Adequacy. Plaintiff and her counsel will fairly and adequately represent the interests of the Class members. Plaintiff has no interests antagonistic to, or in conflict with, the interests of the Class members. Plaintiff's lawyers are highly experienced in the prosecution of consumer class actions and complex litigation.

63. Superiority. A class action is superior to all other available methods for fairly and efficiently adjudicating the claims of Plaintiff and the Class members. Plaintiff and the Class members have been harmed by Anthem's wrongful actions and/or inaction. Litigating this case as a class action will reduce the possibility of repetitious litigation relating to Anthem's wrongful actions and/or inaction.

64. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

65. Class certification also is appropriate under Fed. R. Civ. P. 23(b)(2) because Anthem has acted or refused to act on grounds generally applicable to the Class, so that final

injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

66. The expense and burden of litigation would substantially impair the ability of Plaintiff and Class members to pursue individual lawsuits to vindicate their rights. Absent a class action, Anthem will retain the benefits of its wrongdoing despite its serious violations of the law.

COUNT I

Negligence

(On Behalf of Plaintiff Leniski and the Nationwide Class)

67. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

68. By accepting Plaintiff's and Class members' non-public personal information, Anthem assumed a duty to use reasonable and, at the very least, industry-standard care to secure such information against theft and misuse.

69. Anthem breached its duty of care by failing to adequately secure and protect Plaintiff's and the Class members' personal information from theft, collection and misuse by third parties.

70. Anthem further breached its duty of care by failing to promptly, clearly, accurately, and completely inform Plaintiff and the Class that their personal information had been stolen.

71. Anthem further breached its duty of care by failing to purge and delete records related to former Anthem customers.

72. Plaintiff and the Class have suffered injury in fact, including monetary damages, and will continue to be injured and incur damages as a result of Anthem's negligence and misconduct

73. As a direct and proximate result of Anthem's failure to take reasonable care and use at least industry-standard measures to protect the personal information placed in its care, and failure to purge and delete the information relating to former customers, Plaintiff and members of the Class had their personal information stolen, causing direct and measurable monetary losses,

threat of future losses, identity theft and threat of identity theft.

74. As a direct and proximate result of Anthem's negligence and misconduct, Plaintiff and the Class were injured in fact by: identity theft; damage to credit scores and credit reports; time and expense related to: (a) finding fraudulent accounts; (b) monitoring their identity; (c) credit monitoring and identity theft prevention; (d) income tax refund fraud and the potential for income tax refund fraud; (e) the general nuisance and annoyance of dealing with all these issues resulting from the Anthem data breach; and (f) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the Anthem data breach, all of which have an ascertainable monetary value to be proven at trial.

COUNT II

Negligence *per se*

(On Behalf of Plaintiff Leniski and the Nationwide Class)

75. Plaintiff realleges and incorporates by reference the allegations contained in the preceding paragraphs.

76. Pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. §6801, Anthem had a duty to keep and protect the personal information of its customers.

77. Anthem violated the Gramm-Leach-Bliley Act by failing to keep and protect Plaintiff's and Class members' personal and financial information, failing to monitor, and/or failing to ensure that Defendant complied with data security standards, industry standards, statutes and/or other regulations to protect such personal and financial information.

78. Anthem's failure to comply with the Gramm-Leach-Bliley Act, and/or other industry standards and regulations, constitutes negligence *per se*.

79. Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security and Privacy Rules, 42 U.S.C. §1320d, et seq., Anthem had a duty to keep and protect the personal information of its customers.

80. Anthem violated HIPAA by failing to keep and protect Plaintiff's and Class members' personal and financial information, failing to monitor, and/or failing to ensure that

Defendant complied with PCI data security standards, statutes and/or other regulations to protect such personal and financial information.

81. Anthem's failure to comply with HIPAA, and/or other industry standards and regulations, constitutes negligence *per se*.

COUNT III

Breach of Implied Contract

(On Behalf of Plaintiff Leniski and the Nationwide Class)

82. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 66 above.

83. Plaintiff and the Class provided their financial and personal information to Anthem in exchange for Anthem's services. Plaintiff and members of the Class entered into implied contracts with Anthem pursuant to which Anthem agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class members that their data had been breached and compromised.

84. Each purchase for Anthem's services made by Plaintiff and members of the Class were made pursuant to the mutually agreed upon implied contract with Anthem under which Anthem agreed to safeguard and protect Plaintiff's and Class members' personal and financial information, and to timely and accurately notify them that such information was compromised and breached.

85. Plaintiff and Class members would not have provided and entrusted their financial and personal information to Anthem in order to purchase Anthem services in the absence of the implied contract between them and Anthem.

86. Plaintiff and members of the Class fully performed their obligations under the implied contracts with Anthem.

87. Anthem breached the implied contracts with Plaintiff and members of the class.

///

///

COUNT IV

Breach of Contract

(On Behalf of Plaintiff Leniski and the Nationwide Class)

88. Plaintiff reallages and incorporates by reference the allegations contained in paragraphs 1 through 66 above.

89. Anthem provides health insurance to Plaintiff and members of the Class pursuant to insurance contracts:

a) Plaintiff and members of the Class were either parties to, or third-party beneficiaries of, these insurance contracts.

b) As consideration under the insurance contracts, Plaintiff and members of the Class paid or had paid on their behalf insurance premiums, amounting to thousands of dollars paid annually by or on behalf of each plan member.

c) These insurance contracts explicitly or implicitly incorporate statements made in Anthem's Privacy Policy or on its website that Defendant would safeguard and protect Plaintiff's and Class Members' PHI. Anthem's Notice of Privacy Practices states:

> We are dedicated to protecting your PHI, and have set up a number of policies and practices to help make sure your PHI is kept secure. We keep your oral, written and electronic PHI safe using physical, electronic, and procedural means. These safeguards follow federal and state laws. Some of the ways we keep your PHI safe include securing offices that hold PHI, password-protecting computers, and locking storage areas and filing cabinets. We require our employees to protect PHI through written policies and procedures. These policies limit access to PHI to only those employees who need the data to do their job. Employees are also required to wear ID badges to help keep people who do not belong out of areas where sensitive data is kept. Also, where required by law, our affiliates and nonaffiliates must protect the privacy of data we share in the normal course of business. They are not allowed to give PHI to others without your written OK, except as allowed by law.

90. Pursuant to their insurance contracts, Plaintiff and Class Members paid Anthem to, *inter alia*, safeguard and protect their PHI.

91. Anthem did not safeguard or protect Plaintiff's and Class Members' PHI as required by the insurance contracts.

92. Because Anthem did not safeguard and protect Plaintiff's and Class Members' PHI as promised, Plaintiff and Class Members overpaid for their insurance premiums and have been (and continue to be) damaged.

93. Because Anthem did not safeguard and protect Plaintiff's and Class Members' PHI as promised, Plaintiff and Class Members did not receive the full value of their insurance contracts and have been (and continue to be) damaged.

94. Additionally, as a result of Anthem's breach of contract, Plaintiff and Class members were (and continue to be) injured and have suffered (and will continue to suffer) the damages.

COUNT V

Breach of Fiduciary Duty

(On Behalf of Plaintiff Leniski and the Nationwide Class)

95. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 66 above.

96. Plaintiff and the members of the class, as consumers of medical services from healthcare providers, reposed trust and confidence in their providers at all times material. In order to receive payment for medical care, Plaintiff and the members of the class were required to provide their health care providers with private and confidential information.

97. In order to secure health care coverage from Defendants, Plaintiff and the members of the class were required to permit health care professionals and entities to provide their confidential medical information to the Defendants, and were required to provide their social security numbers and personal identifying information, on a confidential basis.

98. Defendants, in turn, were given access to such personal confidential medical and financial information which they stored and maintained, ostensibly in confidence, and which they were required to strictly maintain in confidence without public access or other disclosure absent the patients' written consent.

99. Plaintiff and the members of the class reposed absolute trust and confidence in their health care providers and insurers – the Defendants – with respect to their medical and related personal financial information, and with respect to Defendants' ongoing maintenance of that information in confidence, without secretion or divulgence absent their express written consent. They had no choice but to provide Defendants access to their confidential and private medical and related financial information, including their social security numbers, in order to receive the benefits of being insured: a necessary benefit to securing treatment or otherwise maintaining good health and well being and receiving appropriate medical attention from their health care providers.

100. Defendants, as health insurers, owe a fiduciary duty to Plaintiff and the members of the class. And by virtue of their position as health care insurers wielding considerable power and virtually unbridled access to personal and confidential information, and because of their superior knowledge, business responsibilities and duties – including those provided by law or statute – and their absolute ability to control or otherwise manipulate the patients' data in their system, Defendants assumed a fiduciary duty to Plaintiff and the members of the class to secure and maintain the personal and confidential information that they received, free from unauthorized intrusion, theft or other disclosure.

101. As a result of this relationship of trust and confidence, the highly confidential nature of the records and data pertaining to medical and financial information, and Defendants' duties and obligations respecting maintaining the privacy of such information, Defendants owed to Plaintiff and the members of the class, the highest degree of loyalty, honesty, fidelity, trust and due care in their fiduciary obligations with respect to the privacy of personal data in Defendants' possession. In order to comport with such duty, Defendants were required to use their utmost ability to protect, preserve and secure such private data and confidential information from unauthorized access to or theft from Defendants' data systems, and take all necessary steps in order to do so, including encrypting such information, and deploying sufficient data access security controls, in order to frustrate and disable hackers or criminals from accessing such

information for their personal profit or unlawful goals.

102. As set forth above, Defendants breached their fiduciary duty to Plaintiff and the members of the class by failing to take all adequate and necessary steps to preserve, secure and maintain the confidentiality and privacy of medical information and financial data. In addition, Defendants breached their fiduciary duties to Plaintiff and the members of the class by failing to timely, fully and adequately disclose the fact that they had not taken the necessary steps to protect such information from unauthorized access and theft and that such information was at a heightened risk of breach by virtue of Defendants' data security failings and policies.

103. Defendants recklessly or knowingly breached their fiduciary duty and consciously created an environment that made Anthem's valuable data systems open prey to criminal hackers and thieves. Alternatively, and without prejudice to the foregoing, Defendants also breached their fiduciary duty by placing their own desire to achieve greater profits ahead of the privacy and data security interests of Plaintiff and members of the class.

104. As a direct and proximate result of Defendants' violations of their fiduciary duty, Plaintiff and members of the class have been injured and have suffered and will continue to suffer economic and non-economic losses in an amount to be determined according to proof at trial.

COUNT VI

Unjust Enrichment

(On Behalf of Plaintiff Leniski and the Nationwide Class)

105. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 66 above.

106. Plaintiff and Class members conferred a monetary benefit on Anthem in the form of monies paid for the purchase of services during the period of the Anthem data breach.

107. Anthem appreciates or has knowledge of the benefits conferred directly upon it by Plaintiff and members of the Class.

108. The monies paid for the purchase of services by Plaintiff and members of the Class to Anthem during the period of the Anthem data breach were supposed to be used by Anthem, in

part, to pay for the administrative and other costs of providing reasonable data security and protection to Plaintiff and members of the Class.

109. Anthem failed to provide reasonable security, safeguards and protection to the personal and financial information of Plaintiff and Class members and as a result, Plaintiff and Class members overpaid Anthem for the services purchased during the period of the Anthem data breach.

110. Under principles of equity and good conscience, Anthem should not be permitted to retain the money belonging to Plaintiff and members of the Class, because Anthem failed to provide adequate safeguards and security measures to protect Plaintiff's and Class members' personal and financial information that they paid for but did not receive.

111. As a result of Anthem's conduct as set forth in this Complaint, Plaintiff and members of the Class suffered damages and losses as stated above, including monies paid for Anthem services that Plaintiff and Class members would not have purchased had Anthem disclosed the material fact that it lacked adequate measures to safeguard customers' information and had Anthem provided timely and accurate notice of the data breach, and including the difference between the price they paid for Anthem's services as promised and the actual diminished value of its services.

112. Plaintiff and the Class have conferred directly upon Anthem an economic benefit in the nature of monies received and profits resulting from sales and unlawful overcharges to the economic detriment of Plaintiff and the Class.

113. The economic benefit, including the monies paid and the overcharges and profits derived by Anthem and paid by Plaintiff and members of the Class, is a direct and proximate result of Anthem's unlawful practices as set forth in this Complaint.

114. The financial benefits derived by Anthem rightfully belong to Plaintiff and members of the Class.

115. It would be inequitable under established unjust enrichment principles of the states where Anthem conducts business for Anthem to be permitted to retain any of the financial

benefits, monies, profits, and overcharges derived from its unlawful conduct as set forth in this Complaint.

116. Anthem should be compelled to disgorge into a common fund for the benefit of Plaintiff and the Class all unlawful or inequitable proceeds received by Anthem.

117. A constructive trust should be imposed upon all unlawful or inequitable sums received by Anthem traceable to Plaintiff and the Class.

118. Plaintiff and the Class have no adequate remedy at law.

COUNT VII

Violation of Indiana Code § 24-5-0.5, *et seq*.

(On Behalf of Plaintiff Leniski and the Nationwide Class)

119. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 66 above.

120. As a citizen of Indiana, Anthem is subject to Indiana law in its dealings throughout the United States.

121. Indiana prohibits a person from engaging in deceptive acts, which are specifically defined in relevant part as representations:

> (1) That such subject of a consumer transaction has . . . characteristics . . . it does not have which the supplier knows or should reasonably know it does not have.
>
> (2) That such subject of a consumer transaction is of a particular standard, quality, grade, style, or model, if it is not and the supplier knows or should reasonably know that it is not.
>
> (6) That a specific price advantage exists as to such subject of a consumer transaction, if it does not and if the supplier knows or should reasonably know that it does not.

IND. CODE § 24-5-0.5-3(a). A "consumer transaction" includes, *inter alia*, the sale, lease or assignment of personal property, real property or a service for purposes that are primarily

personal. IND. CODE § 24-5-0.5-2(1). "Person" includes a corporation. IND. CODE § 24-5-0.5-2(2). "Supplier" is a seller or other person who regularly engages in or solicits consumer transactions and includes a manufacturer "whether or not the person deals directly with the consumer." IND. CODE § 24-5-0.5-2(a)(3).

122. The statute is to be liberally construed and applied to promote its purposes, which are to "(1) simplify, clarify, and modernize the law governing deceptive and unconscionable consumer sales practices; (2) protect consumers from suppliers who commit deceptive and unconscionable sales acts; and (3) encourage the development of fair consumer sales practices." IND. CODE § 24-5-0.5-1(a), (b). 101. For the reasons discussed above, Anthem violated (and, on information and belief, continues to violate) § 24-5-0.5 by engaging in the above-described and prohibited unlawful, unfair, fraudulent, deceptive, untrue, and misleading acts and practices.

123. Anthem violated § 24-5-0.5 by accepting and storing Plaintiff's and the Class members' personal and financial information but failing to take reasonable steps to protect it. In violation of industry standards and best practices, Anthem also violated consumer expectations to safeguard personal and financial information and failed to tell consumers that it did not have reasonable and best practices, safeguards and data security in place. Anthem deceived Plaintiff and the Class by asserting that "[w]e keep the health and financial information of our current and former members private, as required by law, accreditation standards and our rules," and assuring Plaintiff and the Class that "[w]e are dedicated to protecting your PHI, and have set up a number of policies and practices to help make sure your PHI is kept secure."

124. Anthem also violated § 24-5-0.5 by failing to immediately notify Plaintiff and the Class of the Anthem data breach. If Plaintiff and the Class had been notified in an appropriate fashion, they could have taken precautions to better safeguard their personal and financial information.

125. "A person relying upon an uncured or incurable deceptive act may bring an action for the damages actually suffered as a consumer as a result of the deceptive act or five hundred dollars ($500), whichever is greater." IND. CODE § 24-5-0.5-4(a). An "uncured deceptive act" occurs when a consumer who has been damaged gives pre-suit notice and the defendant fails to

cure. IND. CODE § 24-5-0.5-2(a)(7). An "incurable deceptive act" is one "done by a supplier as part of a scheme, artifice, or device with intent to defraud or mislead." IND. CODE § 24-5-0.52(a)(8). Anthem's actions as alleged herein constitute "incurable deceptive acts." If the defendant is found to have acted willfully, the Court may treble the damages or award $1,000, whichever is greater. IND. CODE § 24-5-0.5-4(a).

126. On information and belief, Anthem's unlawful, fraudulent, and unfair business acts and practices, except as otherwise indicated herein, continue to this day and are ongoing. As a direct and/or proximate result of Anthem's unlawful, unfair, and fraudulent practices, Plaintiff and the Class have suffered injury in fact and lost money in connection with the Anthem data breach, for which they are entitled to compensation – as well as restitution, disgorgement, and/or other equitable relief. Plaintiff and the Class were injured in fact by: unauthorized activity on their accounts; damage to credit scores and credit reports; time and expense related to: (a) finding fraudulent charges; (b) cancelling and reissuing cards; (c) credit monitoring and identity theft prevention; (d) imposition of withdrawal and purchase limits on compromised accounts; (e) inability to withdraw funds held in linked checking accounts; (f) trips to banks and waiting in line to obtain funds held in limited accounts; (g) resetting automatic billing instructions; (h) late fees and declined payment fees imposed as a result of failed automatic payments; (i) the general nuisance and annoyance of dealing with all these issues resulting from the Anthem data breach; and (j) costs associated with the loss of productivity from taking time to ameliorate the actual and future consequences of the Anthem data breach, all of which have an ascertainable monetary value to be proven at trial. Plaintiff and the Class are entitled to the greater of their damages as alleged herein or the statutory sum of $500.

COUNT VIII

Violation of the Gramm-Leach-Bliley Act as Unlawful Deceptive Acts and Practices

(On Behalf of Plaintiff Leniski and the Nationwide Class)

127. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1 through 66 above.

128. Defendants have a duty pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. §6801, *et seq.*, and 16 C.F.R. §313, *et seq.*, not to misuse or inappropriately disclose information received as a third party for the purpose of processing a transaction requested by a customer of its stores.

129. Pursuant to 16 C.F.R. §313.11(iii), third party recipients of financial data such as Defendants, cannot "use" or "disclose" the information other than in "the ordinary course of business to carry out the activity covered by the exception under which [it] received the information."

130. Defendants were obligated under 16 C.F.R. §313.11 to *only* use and disclose customer financial information for the purposes for which it was disclosed, more specifically, to process the transaction.

131. Plaintiff, in the course of business, placed her nonpublic, personal information with Defendants, with the expectation that Defendants would access that information only for the purpose of transactions that are initiated by that customer.

132. Defendants violated the Gramm-Leach-Bliley Act in that they improperly used and disclosed the information in violation of the Privacy Regulations by (i) maintaining the data well beyond the permitted time-frame; and (ii) allowing the data to be accessed by criminal hackers for purposes unrelated to the healthcare of Plaintiff and the members of the Class.

133. The acts and practices described above were knowingly unfair and deceptive. Plaintiff and members of the Class have suffered damages as set forth above as a result of these unfair and deceptive trade practices.

COUNT IX

For Injunctive Relief

(On Behalf of Plaintiff Leniski and the Nationwide Class)

134. Plaintiff re-alleges and incorporates by reference the allegations contained in paragraphs 1 through 66 above.

135. On information and belief, Anthem's unlawful, fraudulent and unfair acts and

practices and violations of statutory duties, continue to this day and are ongoing. As a direct and/or proximate result of Anthem's unlawful, unfair and fraudulent practices and violations of statutory duties, Plaintiff and the Class have suffered injury and are at significant risk of suffering future injury and harm.

136. Plaintiff and the Class are entitled to injunctive relief to stop Anthem's continuing wrongful acts and practices and require Anthem to adopt, implement and maintain all adequate and necessary security measures and best practices, including encryption, among other things, to safeguard and protect the personal and financial information in its possession, custody and control, including with respect to its network of healthcare providers and licenses that are permitted to access such information.

137. Plaintiff and the Class are also entitled to injunctive relief to attempt to prevent on-going use of their personal data that was hacked, including lifetime credit and identity theft monitoring and protection.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests the following relief:

A. That the Court certify this case as a class action and appoint the named Plaintiff to be Class representative and her counsel to be Class counsel;

B. That the Court award Plaintiff and the Class appropriate relief, to include actual and statutory damages, disgorgement, and restitution;

C. That the Court award Plaintiff and the Class preliminary or other equitable or declaratory relief as may be appropriate by way of applicable state or federal law;

D. Such additional orders or judgments as may be necessary to prevent these practices and to restore to any person in interest any money or property which may have been acquired by means of the violations; and

E. That the Court award Plaintiff and the Class such other, favorable relief as may be available and appropriate under law or at equity.

///

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all issues so triable.

DATED: June 26, 2015

Respectfully submitted,

Eve H. Cervantez (164709)
Jonathan Weissglass (185008)
ALTSHULER BERZON LLP

/s/ Eve H. Cervantez
EVE H. CERVANTEZ

177 Post Street, Suite 300
San Francisco, CA 94108
Telephone: (415) 421-7151
Facsimile: (415) 362-8064

Stephen R. Basser (121590)
Samuel M. Ward (216562)
BARRACK, RODOS & BACINE
600 West Broadway, Suite 900
San Diego, CA 92101
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

Lisa M. Port
BARRACK, RODOS & BACINE
3300 Two Commerce Square
2001 Market Street
Philadelphia, PA 19103
Telephone: (215) 963-0600
Facsimile: (215) 963-0838

J. Gerard Stranch, IV
Michael Stewart
Karla Campbell
BRANSTETTER, STRANCH AND JENNINGS, PLLC
227 Second Avenue North
Nashville, TN 37201
Telephone: (615) 254-8801
Facsimile: (615) 250-3937
Attorneys for Plaintiff Kathryn Leniski and the Proposed Class